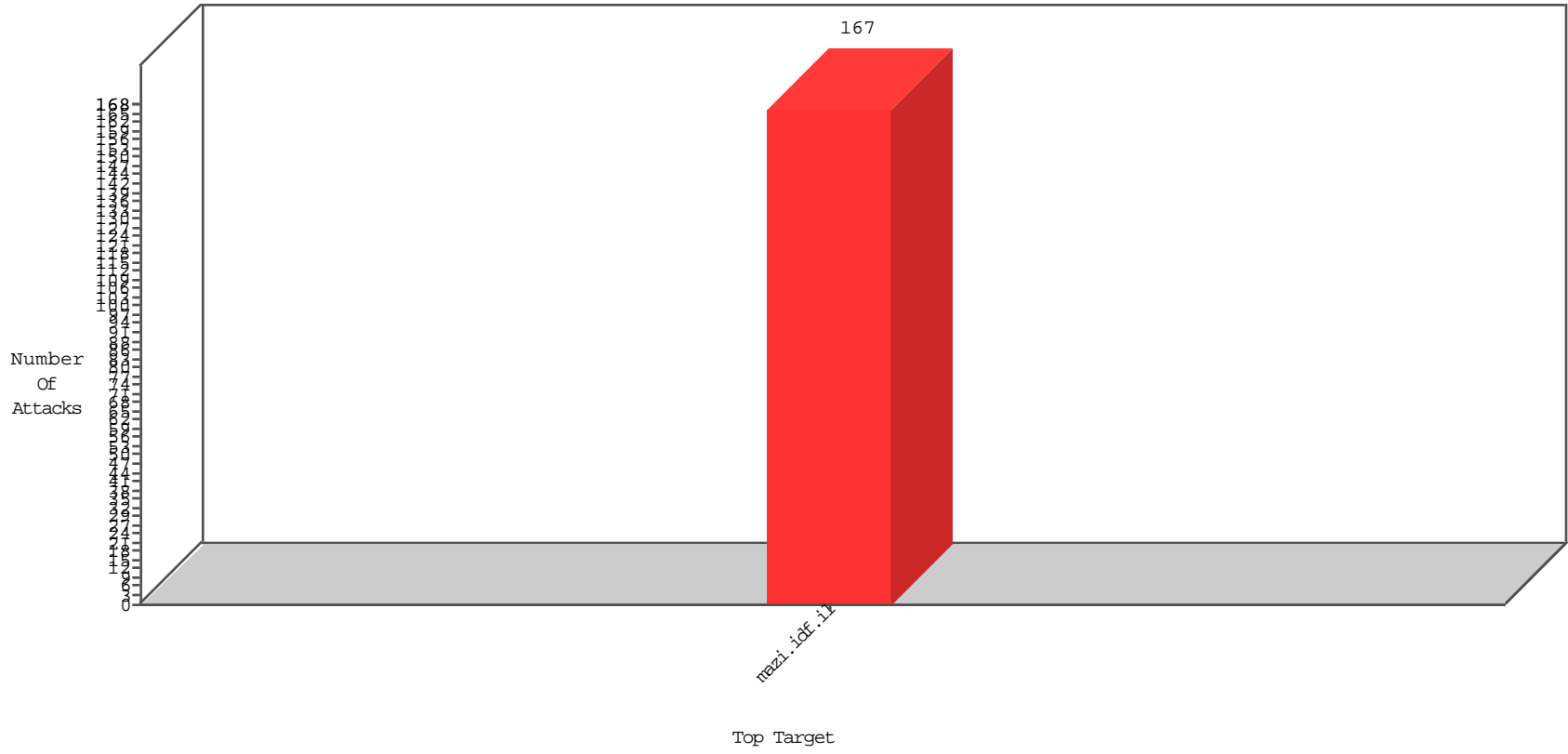


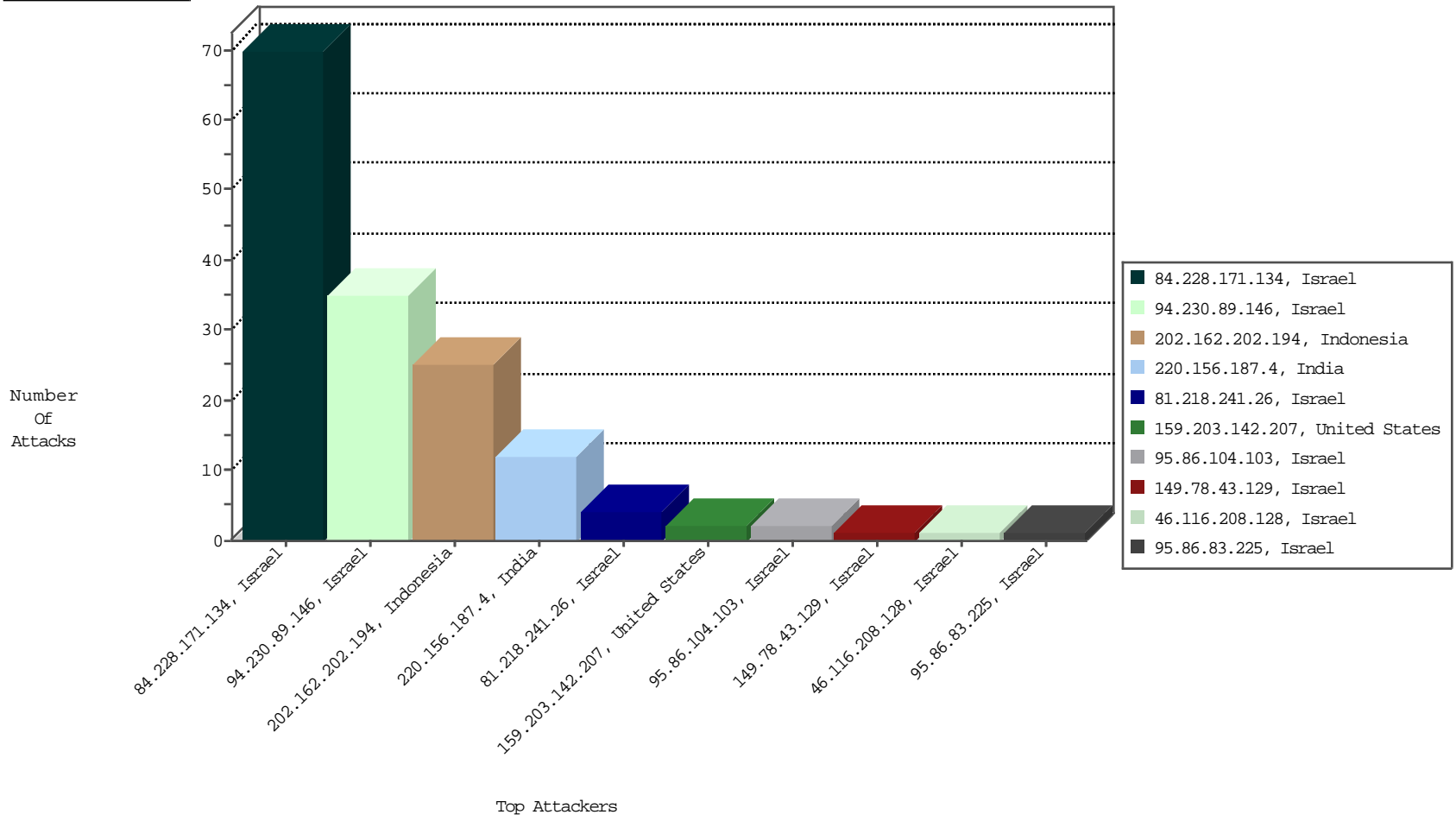
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



01-31-2016 to 02-01-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
142.54.160.214	United States	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BBL-Frankfurt	1

01-31-2016 to 02-01-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	12
202.162.202.194	Indonesia	147.237.77.17	mazi.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	2

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
202.162.202.194	Indonesia	147.237.77.17	mazi.idf.il	SERVER-WEBAPP admin.php access	2
168.62.238.153	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
84.228.171.134	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	3736
94.230.89.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	100
46.19.86.251	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
79.127.43.56	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
79.127.43.56	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	14
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	12
8.37.227.69	Anonymous Proxy	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	9
5.28.135.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
109.67.203.227	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
82.166.240.203	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.177.177	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
37.46.38.93	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.130.77	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.129	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
213.8.95.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
5.28.135.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
157.55.39.129	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.116.208.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.159	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
87.68.40.94	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
191.232.136.140	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.229.132.144	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.116.208.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.223.241	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
2.54.177.177	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
8.37.227.68	Anonymous Proxy	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	4
46.116.208.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
5.29.223.241	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.13.134	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
94.230.86.205	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
212.76.127.4	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
109.64.119.56	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.149.147	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.200.65.67	Ukraine	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.118.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
64.125.239.153	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.120.246.247	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
109.253.223.145	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.254	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
96.250.65.141	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.196		147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Masscan Port Scanner	reject	1

01-31-2016 to 02-01-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.228.171.134	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 84.228.171.134	Block	69
94.230.89.146	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 94.230.89.146	Block	35
202.162.202.194	Indonesia	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 202.162.202.194	Block	15
81.218.241.26	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
202.162.202.194	Indonesia	147.237.77.17	mazi.idf.i	PHP Attempt	Block	4
202.162.202.194	Indonesia	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 202.162.202.194	Block	2
95.86.104.103	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
141.212.122.81	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /x	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL /14-he/igf.aspx[#20]].	Block	1
159.203.142.207	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslist/newslist.in.aspxundefined	Block	1
46.19.86.251	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/6547-he/igf.aspx	Block	1
191.232.136.96	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
95.86.83.225	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
149.78.43.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
84.228.171.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wepdwukltqznjg2mjeIn2rk	Block	1
46.116.208.128	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
192.116.190.250	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
78.110.173.202	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
159.203.142.207	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 159.203.142.207	Block	1
91.228.248.251	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1

01-31-2016 to 02-01-2016